Release Notes for the OmniSwitch 8800: Release 5.1.3.R02

These Release Notes accompany Release 5.1.3.R02 software and OmniSwitch 8800 hardware. They provide important information on individual software features and hardware modules. Since much of the information in these Release Notes is not included in the hardware and software user manuals it is important that you read all sections of this document before installing new hardware or loading new software.

Contents

- Related Documentation, see page 2.
- System Requirements, see page 3.
- New Hardware, see page 4.
- New Software Features, see page 5.
- Unsupported Software Features, see page 6.
- New Hardware Descriptions, see page 15.
- New Software Feature Descriptions, see page 17.
- Open Problem Reports and Feature Exceptions, see page 19.
  - Switch Management, see page 19.
  - Layer 2, see page 22.
  - Layer 3, see page 26.
  - Quality of Service, see page 28.
  - Advanced Routing, see page 30.
  - Authentication and Security, see page 31.
  - System, see page 32.
- Technical Support, see page 37.

Copyright 2003 Alcatel Internetworking, Inc.

Related Documentation

These Release Notes should be used in conjunction with the OmniSwitch 8800 user documentation set. The following are the titles and descriptions of the OmniSwitch 8800 user manuals:

- *OmniSwitch 8800 Getting Started Guide*

  Describes the hardware and software procedures for getting an OmniSwitch 8800 up and running. Also provides information on fundamental aspects of OmniSwitch software architecture.

- *OmniSwitch 8800 Hardware User Guide*

  Complete technical specifications and procedures for all OmniSwitch 8800 chassis', power supplies, fans, and Network Interface (NI) modules.

- *OmniSwitch CLI Reference Guide*

  Complete reference to all CLI commands supported on the OmniSwitch 8800. Includes syntax definitions, default values, examples, usage guidelines and CLI-to-MIB variable mappings.

- *OmniSwitch 7700/7800/8800 Switch Management Guide*

  Includes procedures for readying an individual switch for integration into a network. Topics include the software directory architecture, software rollback protections, authenticated switch access, managing switch files, system configuration, using SNMP, and using web management software (WebView).

- *OmniSwitch 7700/7800/8800 Network Configuration Guide*

  Includes network configuration procedures and descriptive information on all the major software features and protocols included in the base software package. Chapters cover Layer 2 information (Ethernet and VLAN configuration), Layer 3 information (routing protocols, such as RIP and IPX), security options (authenticated VLANs), Quality of Service (QoS), link aggregation, and server load balancing.

- *OmniSwitch 7700/7800/8800 Advanced Routing Configuration Guide*

  Includes network configuration procedures and descriptive information on all the software features and protocols included in the advanced routing software package. Chapters cover multicast routing (DVMRP and PIM-SM), and OSPF.

- *OmniSwitch 7700/7800/8800* Technical Tips, Field Notices

  Contracted customers can visit our customer service website at: http://eservice.ind.alcatel.com.

System Requirements

Memory Requirements

- OmniSwitch 8800 Release 5.1 requires 128 MB of SDRAM and 32MB of flash memory. This is the standard configuration shipped on a Chassis Management Module (CMM).

Configuration files and the compressed software images--including web management software (WebView) images--are stored in flash memory.

Power Supply Requirements

The OmniSwitch 8800 power supply requirements will vary depending on the number of Network Interface (NI) modules installed in the switch and your power redundancy requirements. Each chassis contains 4 slots for power supplies. Please consult the *OmniSwitch 8800 Hardware User Guide* for further information.

The updated power consumption figures below supersede the figures currently in the *OmniSwitch 8800 Hardware User Guide:*

Board	Power Consumption
OS8-ENI-C24	44W
OS8-GNI-C8	143W
OS8-GNI-U8	135W
OS8800-CMM	24W
OS8800-SFM	60W
OS8800 (Chassis: Fan & Blower Trays)	332W

Please consult the *OmniSwitch 8800 Hardware User Guide* for further information.

New Supported Hardware

Chassis/Module Type	Description	Images Required
OS8800	**18-slot chassis**	**n/a**
OS8800-CMM	**Management module for OS8800**	**Ebase.img, Eos.img**
OS8800-SFM	**Fabric Board for OS8800**	**Eeni.img**
OS8-ENI-C24	**24-port 10/100 copper Ethernet for OS8800**	**Eeni.img**
OS8-GNI-C8	**8-port copper Gig Ethernet for OS8800**	**Eeni.img**
OS8-GNI-U8	**8-port universal Gig Ethernet for OS8800**	**Eeni.img**

New Supported Software Features

The following new software features are supported subject to the feature exceptions and problem reports described in "Open Problem Reports and Feature Exceptions" starting on page 19.

Software Feature	Software Package	Image(s) Required
High Availability VLANs	**Base**	**Ebase.img**
Learned Port Security (Configuration lost after takeover)[a]	**Base**	**Eeni.img, Eethl2.img**
Local Proxy Arp	**Base**	**Eeni.img**
Per-VLAN DHCP Servers[a]	**Base**	**Ebase.img**
Policy-Based Routing	**Base**	**Eqos.img**
Secure Shell (SSH)	**Base**	**Ebase.img**

a. Contact Customer Support for Latest Information

Unsupported Software Features

CLI commands and web management options are available in the switch software for the following features. However these features are not supported in the current release.

Software Feature	Software Package
BGP4	**Base**
End User Partitioning	**Base**
Learned Port Security (Configuration lost after takeover)[a]	**Base**
Per-VLAN DHCP Servers[a]	**Base**
User-Defined (Custom) VLAN Rules	**Base**

a. Contact Customer Support for Latest Information

Note. Use of these features in a network with this software release may lead to unpredictable results

Unsupported CLI Commands

The following CLI commands are not supported in this release of the software.

Software Feature	Unsupported CLI Commands
BGP4	**All BGP4 CLI Commands are Unsupported**
Chassis Mac Server	**mac-range local** **mac-range duplicate-eeprom** **mac-range allocate-local-only** **show mac-range status**
End User Partitioning	**All End User Partitioning CLI Commands are Unsupported**
Hot Swap	**reload ni [slot] #**
IPX	**ipx watchdog-spoof [vlan] [enable | disable]** **no ipx watchdog-spoof [vlan]** **show ipx watchdog-spoof** **ipx serialization [vlan] [enable | disable]** **no ipx serialization [vlan]** **show ipx serialization** **ipx spx-spoof [vlan] [enable | disable]** **no ipx spx-spoof [vlan]** **show ipx spx-spoof**
OSPF	**ip ospf router**
Quality of Service	**qos port <slot/port> [no] maximum default depth** **qos port <slot/port> [no] maximum default buffers** **qos port <slot/port> [no] maximum default bandwidth** **qos port <slot/port> [no] maximum signal bandwidth** **qos port <slot/port> [no] maximum reserve bandwidth** **qos [no] classify fragments**
Redundancy	**reload [secondary] {with no time parameter specified)**
User-Defined (Custom) VLAN Rules	**vlan user** **vlan <vid> router ipx <network> [<rip-sap>] [<ipx-encap>] [timeticks <timetick-value>]=> "triggered" mode in <rip-sap>**

Unsupported MIBs and MIB Variables

The following MIBs are not supported in this release of the software

Software Feature	MIB
BGP4	**All MIBs are unsupported**
End User Partitioning	**All MIBs are unsupported**
Quality of Service (QoS)	**IETF_P_BRIDGE**
User-Defined (Custom) VLAN Rules	**All MIBs are unsupported**

The following Mib Variables are not supported:

MIB NAME: AlcatelIND1Dvmrp

MIB Variables Unsupported
dvmrpInterfaceInterfaceKey dvmrpInterfaceInterfaceKeyVersion

MIB NAME: IETF_BRIDGE (RFC 1493)

MIB Variables Unsupported
dot1dBasePortDelayExceededDiscards dot1dStaticAddress dot1qStaticUnicastTable dot1dStaticReceivePort dot1dStaticAllowedToGoTo dot1dStaticStatus dot2dStatic Table dot1dStaticEntry

MIB NAME: IETF_ENTITY (RFC 2737)

MIB Variables Unsupported	
entPhysicalSoftwareRev	entLogicalIndex
entPhysicalAlias	entLogicalTable
entPhysicalAssetID	entLogicalEntry
entPhysicalIsFRU	entLogicalDescr
EntLPPhysicalIndex	entLogicalType
entLPMappingTable	entLogicalCommunity
entLPMappingEntry	entLogicalTAddress
EntAliasMappingTable	entLogicalDomain
entAliasMappingEntry	entLogicalContexEngineID
EntAliasLogicalIndexOrZero	entLogicalContextName
EntAliasMappingIdentifier	

MIB NAME: IETF_ETHERLIKE (RFC 2665)

MIB Variables Unsupported
dot3StatsAlignmentErrors
dot3StatsFCSErrors
dot3StatsSQETestErrors
dot3StatsEtherChipSet
dot3ControlInUnknownOpcodes
dot3ControlTable
dot3InPauseFrames
dot3OutPauseFrames
dot3PauseTable

MIB NAME: IETF_IF (RFC 2863)

MIB Variables Unsupported	
iflnNUcastPkts	ifRcvAddressAddress
iflnUnknownProtos	ifRcvAddressStatus
ifOutNUcastPkts	ifRcvAddressType
ifOutQLen	ifRcvAddressTable
ifSpecific	ifRcvAddressEntry
ifStackHigherLayer	ifTestld
ifStackLowerLayer	ifTestStatus
ifStackStatus	ifTestType
ifStackLastChange	ifTestResult
ifStackTable	ifTestCode
ifStackEntry	ifTestTable
	ifTestEntry
	ifTestOwner

MIB NAME: IETF_IP_FORWARD_MIB (RFC 2096)

MIB Variables Unsupported	
ipCidrRouteInfo	ipForwardProto
	ipForwardAge
ipForwardTable	ipForwardInfo
ipForwardEntry	ipForwardNextHopAS
ipForwardNumber	ipForwardMetric1
ipForwardDest	ipForwardMetric2
ipForwardMask	ipForwardMetric3
ipForwardPolicy	ipForwardMetric4
ipForwardNextHop	ipForwardMetric5
ipForwardIfIndex	
ipForwardType	*Note: Obsolete - Needs to be Replaced by ipCidrRouteTable*

MIB NAME: IETF_IPMROUTE_STD (RFC 2932)

MIB Variables Unsupported	
ipMRoutePkts	ipMRouteInterfaceInMcastOctets
iMRouteDifferentInIfPackets	ipMRouteInterfaceOutMcastOctets
iMRouteOctets	ipMRouteInterfaceHCInMcastOctets
iMRouteHCOctets	ipMRouteInterfaceHCOutMcastOctets
iMRoutrNextHopPkts	
Note: The mibs above always returns a value of Zero	*Note: The mibs above always returns a value of Zero*
ipMRouteInterfaceTable	ipMrouteScopeNameTable
ipMRouteInterfaceEntry	ipMRouteScopeNameEntry
ipMrouteInterfaceIndex	ipMRouteScopeNameAddress
ipMRouteInterfaceTtl	ipMRouteScopeNameAddressMask
ipMRouteInterfaceProtocol	ipMRouteScopeNameLanguage
ipMRouteInterfaceRateLimit	ipMRouteScopeNameString
	ipMRouteScopeNameDefault
Note: Table Access is Read Only	ipMRouteScopeNameStatus

MIB NAME: IETF_MAU (RFC 2668)

MIB Variables Unsupported	
rpMauTable	rpJackIndex
rpMauEntry	rpJackType
rpMauGroupIndex	ifMauFalseCarriers
rpMauPortIndex	ifMauTypeList
rpMauIndex	ifMauAutoNegCapability
rpMauType	ifMauAiutoNegCapAdvertised
rpMauStatus	ifMauAutoNegCapReceived
rpMauMediaAvailable	broadMauBasicTable
rpMauMediaAvailableStateExits	broadMauBasicEntry
rpMauJabberState	broadMauIfIndex
rpMauJabberStateEnters	broadMauIndex
rpMauFalseCarriers	broadMauXmtRcvSplitType
rpJackTable	broadMauXmtCarrierFreq
rpJackEntry	broadMauTranslationFreq

MIB NAME: IETF_OSPF (RFC 1850)

MIB Variables Unsupported	
ospfAuthType	ospfAreaRangeNet
ospfAreaRangeTable	ospfAreaRangeMask
ospfAreaRangeEntry	ospfAreaRangeStatus
ospfAreaRangeAreaLd	ospfAreaRangeEffect

MIB NAME: IETF_Q_BRIDGE (RFC 2674)

MIB Variables Unsupported	
dot1qFdbTable	dot1qTpGroupTable
dot1qFdbEntry	dot1qTpGroupEntry
dot1qFdbId	dot1qTpGroupAddress
dot1qFdbDynamicCount	dot1qTpGroupEgressPorts
dot1qTpFdbTable	dot1qTpGroupLearnt
dot1qTpFdbEntry	dot1qForwardAllTable
dot1qTpFdbAddress	dot1qForwardAllEntry
dot1qTpFdbPort	dot1qForwardAllPorts
dot1qTpFdbStatus	dot1qForwardAllStaticPorts
dot1qStaticMulticastStatus	dot1qForwardAllForbiddenPorts
dot1qStaticUnicastTable	dot1qForwardUnregisteredTable
dot1qStaticUnicastEntry	dot1qForwardUnregisteredEntry
dot1qStaticUnicastAddress	dot1qForwardUnregisteredPorts
dot1qStaticUnicastReceivePort	dot1qForwardUnregisteredStaticPorts
dot1qStaticUnicastAllowedToGo	dot1qForwardUnregisteredForbiddenPorts
dot1qStaticUnicastStatus	dot1qLearningConstraintsTable
	dot1qLearningConstraintsEntry
	dot1qConstraintVlan
Note: All the tables above are Read-Only	dot1qVLANNumDeletes

MIB NAME: IETF_Q_BRIDGE (RFC 2674)

MIB Variables Unsupported	
ConstraintVlan	dot1qCdot1qVlanStaticEntry
dot1qConstraintSet	dot1qVlanStaticName
dot1qConstraintType	dot1qVlanStaticEgressPorts
dot1qConstraintStatus	dot1qVlanForbiddenEgressPorts
dot1qStaticMuticastTable	dot1qVlanStaticUntaggedPorts
dot1qStaticMuticastEntry	dot1qVlanStaticRowStatus
dot1qStaticMuticastAddress	dot1qNextFreeLocalVlanIndex
dot1qStaticMuticastReceivePort	dot1qPortVlanStatisticsTable
dot1qStaticMuticastStaticEgressPorts	dot1qPortVlanStatisticsEntry
dot1qStaticMuticastForbiddenEgressPorts	dot1qTpVlanPortInFrames
dot1qVlanCurrentTable	dot1qTpVlanPortOutFrames
dot1qVlanCurrentEntry	dot1qTpVlanPortInDiscards
dot1qVlanTimeMark	dot1qTpVlanPortOverflowFrames
dot1qVlanIndex	dot1qTpVlanPortOutOverflowFrames
dot1qVlanFdbId	dot1qTpVlanPortInOverflowDiscards
dot1qVlanCurrentEgressPorts	dot1qTpVlanHCStatisticsTable
dot1qVlanCurrentUntaggedPorts	dot1qTpVlanHCStatisticsEntry
dot1qVlanStatus	dot1qTpVlanHCInFrames
dot1qVlanCreationTime	dot1qTpVlanHCOutFrames
dot1qVlanStaticTable	dot1qTpVlanInDiscards

MIB NAME: IETF_RIPv2 (RFC 1724)

MIB Variables Unsupported	
rip2IfConfDomain	rip2PeerLastUpdate
rip2PeerTable	rip2PeerVersion
rip2PeerEntry	rip2PeerRcvBadPackets
rip2Peeraddress	rip2PeerRcvBadRoutes
rip2PeerDomain	

MIB NAME: IETF_RMON (RFC 2819)

MIB Variables Unsupported		
hostControlTable	hostTimeAddress	hostTopNStatus
hostControlEntry	hostTimeCreationOrder	hostTopNTable
hostControlIndex	hostTimeIndex	hostTopNEntry
hostControlDataSource	hostTimeInPkts	hostTopNReport
hostControlTableSize	hostTimeOutPkts	hostTopNIndex
hostControlLastDeleteTime	hostTimeInOctets	hostTopNAddress
hostControlOwner	hostTimeOutOctets	hostTopNRate
hostControlStatus	hostTimeOutErrors	matrixControlTable
hostTable	hostTimeOutBroadcastPkts	matrixControlEntry
hostEntry	hostTimeOutMulticastPkts	matrixControlIndex
hostAddress	hostTopNControlTable	matrixControlDataSource
hostCreationOrder	hostTopNControlEntry	matrixControlTableSize
hostIndex	hostTopNControlIndex	matrixControlLastDeleteTime
hostInPkts	hostTopNHostIndex	matrixControlOwner
hostOutPkts	hostTopNRateBase	matrixControlStatus
hostInOctets	hostTopNTimeRemaining	matrixDSDestAddress
hostOutOctets	hostTopNDuration	matrixSDTable
hostOutErrors	hostTopNRequestedSize	matrixSDEntry
hostOutBroadcastPkts	hostTopNGrantedSize	matrixSDSourceAddress
hostOutMulticastPkts	hostTopNStartTime	matrixSDIndex
hostTimeTable	hostTopNOwner	matrixSDPkts
hostTimeEntry		matrixSDOctets
		matrixSDErrors

MIB NAME: IETF_RMON (RFC 2819)

MIB Variables Unsupported		
matrixDSTable	channelTable	captureBufferPacketLength
matrixDSEntry	channelEntry	captureBufferPacketTime
matrixDSSourceAddress	channelIndex	captureBufferStatus
matrixDSIndex	channelIfIndex	bufferControlTable
matrixDSPkts	channelAcceptType	bufferControlEntry
matrixDSOctets	channelDataControl	bufferControlIndex
matrixDSErrors	channelTurnOnEventIndex	bufferControlChannelIndex
filterTable	channelTurnOffEventIndex	bufferControlFullStatus
filterEntry	channelEventIndex	bufferControlFullAction
filterIndex	channelEventStatus	bufferControlCaptureSliceSize
filterChannelIndex	channelMatches	bufferControlDownloadSliceSize
filterPktDataOffset	channelDescription	bufferControlDownloadOffset
filterPktData	channelOwner	bufferControlMaxOctetsRequested
filterPktDataMask	channelStatus	bufferControlMaxOctetsGranted
filterPktDataNoMask	captureBufferTable	bufferControlCapturedPackets
filterPktStatus	captureBufferEntry	bufferControlTurnOnTime
filterPktStatusMask	captureBufferControlIndex	bufferControlOwner
filterPktStatusNoMask	captureBufferIndex	bufferControlStatus
filterOwner	captureBufferPacketId	
filterStatus	captureBufferPacketData	

MIB NAME: IETF_RS_232 (RFC 1659)

MIB Variables Unsupported	
rs232PortInSpeed	rs232SyncPortClockSource
rs232PortOutSpeed	rs232SyncPortFrameCheckErrs
rs232PortInFlowType	rs232SyncPortTrnsmitUnderrunErrs
rs232PortOutFlowType	rs232SyncPortReceiveOverrunErrs
rs232AsyncPortBits	rs232SyncPortInterruotedFrames
rs232AsyncPortStopBits	rs232SyncPortAbortedFrames
rs232AsyncPortParity	rs232SyncPortRole
rs232AsyncPortAutobaud	rs232SyncPortEncoding
	rs232SyncPortRTSControl
Note: All the mibs above are read Only	rs232SyncPortRTSCTSDelay
	rs232SyncPortMode
rs232SyncPortTable	rs232SyncPortIdlePattern
rs232SyncPortEntry	rs232SyncPortMinFlags
rs232SyncPortIndex	

MIB NAME: IETF_SNMP_COMMUNITY (RFC 2576)

MIB Variables Not Fully Supported	
snmpCommunityName	snmpTargetAddrExtTable
snmpCommunityContextEngineID	snmpTargetAddrExtEntry
snmpCommunityContextName	snmpTargetAddrTMask
snmpCommunityEntry	snmpTargetAddrMMS
snmpCommunityTable	snmpTrapAddress
snmpCommunityTransportTag	snmpTrapCommunity
snmpCommunityStorageType	

MIB NAME: IETF_SNMP_NOTIFICATION (RFC 2573)

All MIB Variables are Unsupported

MIB NAME: IETF_SNMP_PROXY (RFC 2573)

All MIB Variables are Unsupported

MIB NAME: IETF_SNMP-USER_BASED_SM (RFC 2574)

MIB Variables Not Fully Supported	
usmUserSpinLock	usmUserOwnPrivKeyChange
usmUserCloneFrom	usmUserPublic
usmUserAuthProtocol	usmUserStorageType
usmUserAuthKeyChange	usmUserStatus
usmUserOwnAuthKeyChange	usmUserTable
usmUserPrivProtocol	usmUserEntry
usmUserPrivKeyChange	

MIB NAME: IETF_SNMP_TARGET (RFC 2573))

MIB Variables Not Fully Supported
snmpUnavailableContexts
snmpUnknownContexys

MIB NAME: IETF_SNMP_VIEW_BASED_ACM (RFC 2575)

MIB Variables Not Fully Supported	
vasmGroupName	vacmAccessEntry
vacmSecurityToGroupStorageType	vacmAccessStorageType
vacmSecurityToGroupStatus	vacmAccessStatus
vacmSecurityToGroupTable	vacmViewSpinLock
vacmSecurityToGroupEntry	vacmViewTreeFamilyMask
vacmAccessContextMatch	vacmViewTreeFamilyType
vacmAccessReadViewName	vacmViewTreeFamilyStorageType
vacmAccessWriteViewName	vacmViewTreeFamilyStatus
vacmAccessNotifyViewName	vacmViewTreeFamilyTable
vacmAccessTable	vacmViewFamilyEntry

MIB NAME: IETF_SNMPV2 (RFC 1907)

MIB Variables Not Fully Supported	
sysORLastChange	snmpInGetRequests
sysORTable	snmpInGetNexts
sysOREntry	snmpInSetRequests
sysORIndex	snmpInGetResponses
sysORID	snmpOutTooBigs
sysORUpTime	snmpOutNoSuchNames
snmpTrapOID	snmpOutBadValues
snmpTrapEnterprise	snmpOutGenErrs
snmpInTraps	snmpOutGetRequests
smpInTooBigs	snmpOutGetNexts
snmpInNoSuchNames	snmpOutSetRequests
smpInReadOnlys	snmpOutGetResponses
snmpInGenErrs	snmpOutPkts
snmpInTotalRegVars	snmpOutTraps
snmpInTotalSetVars	

MIB NAME: IETF_TUNNEL (RFC 2667)

MIB Variables Unsupported
tunnelIfEncapsMethod
tunnelIfSecurity
tunnelIfTOS
tunnelConfigEncapsMethod

MIB NAME: IETF_VRRP (RFC 2787)

MIB Variables Unsupported
vrrpOperAuthType

MIB NAME: NOVELL_IPX

MIB Variables Unsupported	
ipxDestServTable	ipxStatisRouteTable
ipxDestServEntry	ipxStatisRouteEntry
ipxDestServSysInstance	ipxStatisRouteSysInstance
ipxDestServNetNum	ipxStatisRouteCircIndex
ipxDestServNode	ipxStatisRouteNetNum
ipxDestServSocket	ipxStatisRouteExistState
ipxDestServName	ipxStatisRouteTicks
ipxDestServType	ipxStatisRouteHopCount
ipxDestServProtocol	
ipxDestServHopCount	*Note: Table has Read Only Support*
ipxStaticServTable	
ipxStaticServEntry	
ipxStaticServSysInstance	
ipxStaticServCircIndex	
ipxStaticServName	
ipxStaticServType	
ipxStaticServExistState	
ipxStaticServNetNum	
ipxStaticServNode	
ipxStaticServSocket	
ipxStaticServHopCount	

MIB NAME: NOVELL_RIPSAP

MIB Variables Unsupported
ripCircPace
ripCircAgeMultiplier
sapCircPace
sapCircAgeMultiplier

Hardware Descriptions

This section includes a description of all new hardware supported in this release.

Chassis

OmniSwitch 8800

The 18-slot OmniSwitch 8800 (OS8800) chassis provides 16 slots for Network Interface (NI) modules and 2 slots for Chassis Management Modules (CMMs). OS8800 chassis provide important availability features, such as hardware redundancy and hot swapping. With the maximum number of NI modules installed, this chassis supports up to 384 10/100 Ethernet ports and up to 128 Gigabit Ethernet ports.

Chassis Management Modules (CMMs)

OS8800-CMM

The Chassis Management Module (CMM) is the management unit for OmniSwitch 8800 switches. In its role as the management unit, the CMM provides key system services, including: console, modem, and Ethernet management port connections to the switch; software and configuration management, including the Command Line Interface (CLI); web-based management (WebView); SNMP management; power distribution; switch diagnostics; availability features, including redundancy (when used in conjunction with another CMM), software rollback, temperature management, and power management.

OS8800-SFM

Switch Fabric Modules (SFMs) provide the store-and-forward switching fabric function for the OmniSwitch 8800. SFMs act as the link between other components on the OmniSwitch 8800, supporting communication among the various NIs and CMMs. A complete switch fabric consists of four SFM modules--which operate together as a single synchronized fabric--plus one optional module for redundancy. SFMs are located in the rear of the switch in numbered slots specifically designed for SFMs. Other NIs or CMMs will not function in SFM slots.

Network Interface Modules (NIs)

OS8-ENI-C24

Provides 24 twisted-pair RJ-45 ports, individually configurable as 10BaseT or 100BaseTX. This module provides the following features: hardware-enhanced Layer 2 switching and Layer 3 routing capacity; bi-directional wire speed switching on all ports; a built-in Queue Manager, providing system buffering, QoS priority, and bandwidth control features; individual NI reload; on-the-fly hot swapping; and support during CMM failover.

OS8-GNI-C8

Provides eight 1000BaseT (1 Gbps) RJ-45 twisted-pair ports. This module can be used for connections to high-speed, high-capacity network servers. It can also be used for backbone connections in networks where Gigabit Ethernet is used as the backbone media.

OS8-GNI-U8

Provides eight MiniGBIC (1 Gbps) slots. A MiniGBIC is an optical transceiver providing a Gigabit Ethernet connectivity that is hot-pluggable—i.e., it can be installed or removed while the GNI is powered on and operating without the risk of damage to the MiniGBIC module or the host circuitry. Alcatel

MiniGBICs are Small Form-factor Pluggable (SFP) MSA (Multi Source Agreement) compliant. Three MiniGBIC types are available for OS8-GNI-U8 modules:

- MiniGBIC-SX: 1000BaseSX multimode fiber, supports distances up to 550 meters; uses an LC connector
- MiniGBIC-LX—1000BaseLX single mode fiber, supports distances up to 10 km; uses an LC connector
- MiniGBIC-LH-70—1000BaseLH single mode long haul fiber, supports distances up to 70 km; uses an LC connector

Software Feature Descriptions

This section includes a description of all new software features included in this release.

High Availability VLANs

High Availability VLANs, unlike standard Alcatel VLANs, allow you to send traffic intended for a single destination address to multiple switch ports. These high availability VLANs can be used to manage third-party sever clusters.

Learned Port Security

Learned Port Security (LPS) provides a mechanism for authorizing source learning of MAC addresses on 10/100 and Gigabit Ethernet ports. The only types of Ethernet ports that LPS does not support are link aggregate and tagged (trunked) link aggregate ports. Using LPS to control source MAC address learning provides the following benefits:

- A configurable source learning time limit that applies to all LPS ports.
- A configurable limit on the number of MAC addresses allowed on an LPS port.
- Dynamic configuration of a list of authorized source MAC addresses.
- Static configuration of a list of authorized source MAC addresses.
- Two methods for handling unauthorized traffic: stopping all traffic on the port or only blocking traffic that violates LPS criteria.

Local Proxy ARP

The proxy ARP feature can be enabled on a per VLAN basis using the vlan local-proxy-arp command. When the Local Proxy ARP feature is enabled, ARP requests return the MAC address of the IP router port defined for the VLAN, and all traffic within the VLAN is routed. This feature is intended for use with port mapping applications where VLANs are one-port connections. This allows hosts on the port mapping device to communicate via the router. ARP packets are still bridged across multiple ports.

Per-VLAN DHCP Servers

The OmniSwitch allows you to configure the UDP Relay feature based on the VLAN ID of the DHCP request. For the Per-VLAN service, you identify the number of the VLAN that makes the relay request.

You may identify one or more server IP addresses to which DHCP packets will be sent from the specified VLAN.

Policy-Based Routing

Policy Based Routing (PBR) uses QoS policies to override the normal routing mechanism (the routing table) in the switch. PBR is used to redirect traffic based on source or destination IP address, source or destination network group, source or destination TCP/UDP port, a service or service group, IP protocol, or built-in source port group.

Traffic may be redirected to a particular gateway regardless of what routes are listed in the routing table; or traffic may be redirected only if no route exists in the routing table.

Secure Shell (SSH)

The Secure Shell feature provides a secure mechanism that allows you to log in to a remote switch, to execute commands on a remote device, and to move files from one device to another. Secure Shell provides secure, encrypted communications even when your transmission is between two untrusted hosts or over an unsecure network.

The OmniSwitch includes both client and server components of the Secure Shell interface and the Secure Shell FTP file transfer protocol. SFTP is a subsystem of the Secure Shell protocol. All Secure Shell FTP data are encrypted through a Secure Shell channel.

When used as an SSH Server, the following SSH Software is supported on the indicated operating systems:

SSH Software	Supported Operating Systems
OpenSSH	Sun Solaris, Win NT + Cygwin, Mac OSX, Linux Red Hat
F-Secure	Sun Solaris, Win 2000, Win NT, Win XP, Mac OS9
SSH-Communication	Sun Solaris, Win 2000, Win NT, Win XP, Linux Red Hat
PuTTY	Win 2000, Win NT, Win XP, Mac OS9
MAC-SSH	Mac OS9, Mac OSX

When used as an SSH Client, the following SSH Software is supported on the indicated operating systems:

SSH Software	Supported Operating Systems
OpenSSH	Sun Solaris, Win NT + Cygwin, Linux Red Hat, AOS
F-Secure	Sun Solaris, Win 2000, Win NT
SSH-Communication	Sun Solaris, Win 2000, Win NT, Win XP, Linux Red Hat

Open Problem Reports and Feature Exceptions

The problems listed here include problems known at the time of the product's release. Any problems not discussed in this section should be brought to the attention of the Alcatel Technical Support organization as soon as possible.

Switch Management

Command Line Interface (CLI)

Problem Reports

PR 68558

Filtering of the output does not ignore the leading spaces. In a table displayed via the **show ip route** command, each row starts with two spaces and any filtering of the rows should consider the spaces as well. In this particular example, the filtering pattern should also start with two spaces: " 4.*" or "*4.*" in place of "4.*".

Workaround: There is no known workaround at this time.

PR 68798

Logging out from a telnet session by any other method than **exit** AND having a CLI timeout session set to a value greater than 4 minutes in case of network outage, will cause the cpu utilization to go to 100%.

Workaround: Do NOT end a telnet session by using <ctr>, bracket and "q" or by closing it from the drop down list at the top bar (close). Type **exit** or set the CLI timeout session to a value of 3 minutes or less so when the timeout session times out in case of a network outage.

SNMP

Problem Reports

PR 53289

Cannot disable the flood multicasting on an interface via SNMP.

Workaround: There is no known workaround at this time.

Web-Based Management (WebView)

Feature Exceptions

- WebView uses signed applets for the automatic IP reconfiguration. Those applets are signed using VeriSign Certificates that expire every year.The certificates used for Internet Explorer and Netscape expires every August. WebView users have to validate a warning indicating that the certificate used by the applet has expired.

Problem Reports

PR 59678

In Netscape, some home pages may display tables misaligned. This is due to Netscape browser having problems aligning tables even though they're coded to have the same alignment -- this is true for all platforms.

Workaround: Scroll down to view all tables.

PR 64458

With WebView, if the aggregate name has a quotation mark in it, all the Aggregates cannot be displayed.

Workaround: Do not use a quotation mark in an Aggregate name.

PR 68151

Validation/Error messages have backslash (\) in front of the apostrophe (').

Workaround: Please ignore the backslashes.

PR 68581

When there is no secondary CMM installed, the LED status page displays ERR(NaN) in the secondary status column.

Workaround: This is only a display issue.

PR 69014

Unable to change the default queue size from the WebView.

Workaround: There is no known workaround at this time.

PR 69313

WebView allows creation of QoS rules using conditions and actions already created from PolicyView. Such creation of rules should not be practiced otherwise after deleting policy conditions and actions from PolicyView, there will be no way to delete corresponding rules from WebView.

Workaround: Use PolicyView created conditions and actions for PolicyView rules, and WebView created conditions and actions for WebView rules.

PR 69333

WebView RIP/RIPv2 Interface Admin Status says "Not In Service" when the **show ip rip interface** CLI command shows enabled or disabled. The i**nterface admin status** command in WebView and CLI are not the same. It is a combination of **Intf Admin status** AND **IP intf status** in CLI . It would be active only if **Intf Admin status** and **IP intf status** are active. If either of them is inactive, WebView shows it as inactive.

Workaround: Interprete the **Interface admin status** command in WebView as **Interface Status**.

PR 69358

In WebView, if an attempt is made to add an IPX filter without completing the entire "add" form, potentially undesirable defaults will be chosen for the filter net and net mask resulting in a bad filter.

Workaround: The net and net mask fields should be explicitly defined before submitting the IPX Filter "Add" form. No fields should be left blank.

PR 69399

In WebView, IPX RIP/SAP table may yield an empty table on the first load of the table. Subsequent reloads of the table will display proper table contents.

Workaround: Reloading or re-navigating to the page will cause the table to display properly.

Layer 2

IP Multicast Switching (IPMS)

Problem Reports

PR 68918

"IPMNI14 13/0 ipmni_commit" related messages might be occasionally seen on the console if multiple subsequent takeovers on the CMMs are performed on the chassis in a short period of time. The impact is that some IP Multicast flows may not recover after a takeover. Stopping the flow for 5 minutes will permit it to be forwarded correctly.

Workaround: Check for the recommended procedures for "Redundancy / Hot Swap" starting on page 34 in the release notes.

PR 69197

"ipmem_desc_add 204" messages might be seen scrolling after hot-insertion of a previously extracted NI with IPMS/R traffic running through the chassis. This might also bring the power down on that particular NI and a reboot of the chassis will be required to recover from this situation.

Workaround: If IPMS/R traffic runs through the chassis, do not hot re-insert the NI that has been recently extracted. Always insert any such NIs by bringing the power down on the chassis first. Fix for this issue soon to be provided in the subsequent maintenance builds.

Learned Port Security

Problem Reports

PR 69320

Learned Port Security configuration is lost after a takeover.

Workaround: There is no known workaround at this time.

Per-VLAN DHCP Servers

Problem Reports

PR 69280

DHCP Requests not relayed when source interface is not local.

Workaround: There is no known workaround at this time.

Port Mirroring

Problem Reports

PR 61468

When mirroring a mobile port, only the VLANs assigned to the source port at the time the mirror was created will be transferred to the target (mirroring) port.

Workaround: When mirroring a mobile port ensure that the VLANs of interest assigned to the port have been established prior to configuring port mirroring.

PR 67418

Port mirroring session cannot be created via SNMP.

Workaround: Use CLI.

PR 69516

Vlan-port changes on mobile ports are not reflected when port mirroring is ON.

Workaround: Configure port mirroring once the mobile port has attained the vlan-port setup required.

Source Learning

Problem Reports

PR 68052

Link aggregation and Learned Port Security should not be configured on the same port. Presently the switch lets the user configure both on the same port.

Workaround: There is no known workaround at this time.

PR 68887

If a mac address is learnt in multiple vlans, the CLI display will show the mac address being learnt only in the first vlan where the switch classified the mac address.

Workaround: This is a display issue and does not affect functionality.

PR 69312

After takeover, the show command for port-mac feature displays incorrect values.

Workaround: There is no known workaround at this time.

Spanning Tree

Problem Reports

PR 62244

During a takeover, some over processing on the NI side may prevent the switch (root bridge) to forward its BPDU. In such a case, the max age timer may trigger on the switch closest to the root bridge, generating a Topology change. After the over processing burst, everything returns back to the initial state.

Workaround: There is no known workaround at this time.

PR 65465

Changing any Spanning Tree parameter on a port for VLAN 1, when VLAN 1 is tagged for that port, is not applied during the execution of the initial configuration file (boot.cfg).

Workaround: Do not use VLAN 1 as a 'tagged' VLAN.

PR 67917

Sometimes, a Listening/Learning state can be observed during a spanning tree topology change (change of the Root port).

Workaround: There is no known workaround at this time.

PR 69261

When the Spanning Tree is disabled, any incoming BPDU are dropped. They are not forwarded on to the other ports that belong to the same Spanning Tree instance.

Workaround: Do not turn off Spanning Tree if there is more than one connection.

VLANs

Problem Reports

PR 61994

When traffic violates a port-protocol binding rule, source learning does not indicate by vlan which rule was violated.

Workaround: There is no known workaround at this time.

PR 66968

On a boot-up, when the switch is routing from a VRRP vlan to a RIP vlan, there might be a delay of 30 seconds before the switch starts to route into the RIP vlan.

Workaround: There is no known workaround at this time.

PR 68249

If a mobile port's default vlan is changed to the vlan it has joined due to configured rules, the traffic on the default vlan is blocked.

Workaround: There is no known workaround at this time.

PR 68968

Switching to a single mode mac router will not deallocate already allocated macs which have been saved in the configuration file.

Workaround: If you are switching to single mode, delete all mac allocation commands from boot.cfg.

PR 69277

Sometimes, a takeover will cause the VLAN manager task to crash.

Workaround: There is no known workaround at this time.

PR 69394

If the NI is removed from the chassis or if the same procedure is done through the “no power ni xx" software command and if there are IP Static/IPX routes they still remain in the IP/IPX forwarding table, the IP/IPX interfaces shows the status as up and the Vlan manager does not report that the NI is down to the IP/IPX protocol.

Workaround: There is no known workaround at this time.

PR 69458

Occasionally, after bootup, on sending 802.1p or ToS/DSCP priority traffic from a port on a slice to another port on the same slice, the user may see that the traffic is not getting prioritized.

Workaround: Disconnect and reconnect the cable to the port to which the traffic is destined.

Layer 3

Basic IP Routing

Problem Reports

PR 68341

Ping with "count 0" is not sending any data out rather than sending it continuously.

Workaround: There is no known workaround at this time.

PR 68667

Fragmentation of IP multicast packets over DVMRP tunnels not supported using SNAP headers.

Workaround: There is no known workaround at this time.

PR 68770

When adding IP VLANs after a static route has been added, the following warning message is seen which does not indicate that the request failed:

SAT DEC 14 16:50:28 : SYSTEM (75) info message:

+++ rtinit: wrong ifa (744d658) was (744d550)

Workaround: There is no known workaround at this time.

PR 68846

Duplicate IP address message does not display IP address in decimal.

Workaround: There is no known workaround at this time.

PR 68867

When the RIP send version is changed from V1 to V2 for an interface, it should be added to the 224.0.0.9 multicast group. This does not seem to happen and so, RIP stops receiving packets on that interface.

Workaround: Disable and Enable the interface status.

IPX

Problem Reports

PR 68826

When using the Ixia ScriptMate, Ixia tries to reacquire the link. It detects a timeout and is unable to pass traffic.

Workaround: Configure Ixia side as non-auto, then there will be no more link changes.

UDP Relay

Problem Reports

PR 55580

When going through the relay, the PXE client is unable to validate the DHCP offer from the server.

Workaround: There is no known workaround at this time.

Quality of Service (includes ACLs and NAT)

Problem Reports

PR 60070

The boot.cfg file can easily become really big when configuring a lot of QoS rules, actions, and conditions. Currently, QoS can handle up to 4096 criterias to classify traffic and apply the QoS actions. However, the switch cannot reboot properly when the boot.cfg has such a large qos configuration.

Workaround: There is no known workaround at this time.

PR 62392

QoS displays zero match count for IP Multicast rules even if they are matched and the IP Multicast policies are enforced.

Workaround: There is no known workaround at this time. It is a display issue only.

PR 65492

When configuring in "reflexive" policy or a "NAT many to one" policy, the condition cannot only be a "destination port slot/port" or a "ip protocol" condition. One has to have at least one "real" Layer3/Layer4 criteria in the condition (source ip or dest ip or source ip port or dest ip port) Of course if the condition combines a "destination port" or "ip protocol" with at least one "real" Layer 3 / Layer 4 criteria, it works fine.

Workaround: Give at least one "real" Layer 3 / Layer 4 criteria in the condition.

PR 68550

When using link aggregation, one cannot use QoS with **destination port slot/port** or **destination interface type** to match the traffic going through the link aggregation. QoS only knows the virtual port of the link aggregation, but does not know anything about the physical port that is used to forward traffic.

Workaround: There is no known workaround at this time.

PR 68555

Every time one does a **qos apply** when the qos configuration has changed, all traffic on the switch will be disturbed. Basically, all hardware entries are flushed and all traffic goes to source learning again. The switch throughput will drop for a short time (software speed instead of wire speed). This means that some packets may be lost depending on the amount of traffic when the **qos apply** command is issued.

Workaround: There is no known workaround at this time.

PR 68818

QOS accepts both "alternate" and "permanent" gateway ips for a PBR action. They should be mutually exclusive.

Workaround: Do not configure both in the same CLI action.

PR 68820

NAT/REFLEXIVE does not work with the src built-in port group, if no Layer3 rules are active on slices seeing reverse traffic.

Workaround: Create a bogus Layer3 rule that is active on the other slots that you're sending traffic.

PR 68863

After several takeovers, QoS queues may not show up on the 'show qos queue' display although they are actually created.

Workaround: There is no known workaround at this time. This is a display issue only.

PR 68906

Sometimes, all the policies do not flush.

Workaround: Issue the **policy server flush** command from the command line to delete all the policies.

PR 68849

Policy->Groups->Ports does not display all built-in port groups.

Workaround: There is no known workaround at this time.

PR 69013

qos classifyl3 bridged enable is equivalent to these two commands: **qos classifyl3 bridged** and **qos enable**.

Workaround: Use **qos no classifyl3 bridge** instead of disable modifier, and use **qos classifyl3 bridged** instead of enable modifier. The modifiers are somewhat misleading that with the command it shows that enable/disable is a legitimate modifier which in fact is not.

PR 69311

Currently, QoS does not support classifications of policy conditions with ToS/DSCP/802.1p. If such a condition is created from WebView/PolicyView, such conditions will not be enforced on the switch. A refusal of such policies will not occur by Policy Manager running on the switch.

Workaround: There is no known workaround at this time.

Advanced Routing

DVMRP

Problem Reports

PR 69042

"tDvmrp" task crash might be occasionally seen if many extended NI hot swaps and re-insertions are performed on a chassis running IPMS/R configuration and multi-cast traffic.

Workaround: If IPMS/R traffic runs through the chassis, do not hot re-insert the NI that has been recently extracted. Always insert any such NIs by bringing the power down on the chassis first.

OSPF

Problem Reports

PR 68589

Consistent route flapping in a large OSPF network (say 20,000 LSAs) may significantly increase CPU utilization.

Workaround: There is no known workaround at this time.

PR 68704

Disabling/Enabling of area range summary not supported.

Workaround: Delete/Create area range summary.

PR 68827

Consistent route flapping in a large OSPF network (say 20,000 LSAs) may significantly increase CPU utilization.

Workaround: There is no known workaround at this time.

PR 69435

In IP / OSPF / Area default metrics, WebView and SNMP will not let a user change both a metric value and its type at the same time.

Workaround: Modify one value at a time.

Authentication and Security

Authenticated Switch Access

Authenticated VLANs

Feature Exceptions

- AVLAN HTTP uses signed applets for the automatic IP reconfiguration. Those applets are signed using VeriSign Certificates that expire every year.The certificates used for Internet Explorer and Netscape expire each August. AVLAN HTTP users have to validate a warning indicating that the certificate used by the applet has expired. A renewed certificate will be applied to the next release.

Problem Reports

PR 68469

Excess files accumulate in the /flash/switch/avlan directory on the OS8800. If many software installations are performed, the excess files will cause the primary to secondary synchronization to fail.

Workaround: Remove files in /flash/switch/avlan immediately before performing an update of the Alcatel switch operating system.

PR 69546

Avlan configurations only support default Class A, B or C type masks.

Workaround: There is no known workaround at this time.

System

Upgrading from 5.1.3 (pre GA builds) on the OmniSwitch 8800 with an FPGA 40

Follow the standard upgrade procedure in the getting started guide, which is in short:

1. FTP the 5.1.3.R02 software to the working directory of the primary.
2. Type **install *.img** and respond to the Fwebsecu.img prompt with a **Y**, if prompted.
3. Type **reload working no rollback-timeout**
4. Type **copy working certified flash-synchro**.
5. Complete. Software is upgraded and the secondary is in hot standby.
6. Type **show running-directory** to confirm.

Feature Exceptions

- When a chassis is fully loaded with 5 modules, an Amber Light indicates that the module is in Stand-By mode.

General

Problem Reports

PR 60142

When priority 2 and priority 3 traffic are sent at wire rate on all 384 ports of the switch, as much as 40% of the traffic may be dropped.

Workaround: Configure the network applications and the switch QoS parameters so that only the highest priority traffic is being sent at priority 3 through the switch.

PR 66379

"State Change Trap not sent - Trap generation failed" NON-FATAL STR which indicates that a Trap failed to be generated because of a resource shortage.

Workaround: There is no known workaround. This is a display issue only.

PR 66781

The Alcatel Operating System does not support non-contiguous MAC ranges.

Workaround: There is no known workaround at this time.

PR 67522

Hardware queues in error state after a link goes up and down. Traffic stops between the bad slot and other slots.

Workaround: Power the NI off and on.

PR 68257

Any open FTP sessions are not closed if a takeover occurs.

Workaround: Exit FTP sessions that were connected to the CMM that has become the secondary. Re-connect to the new primary CMM.

PR 68266

The **show module** command will not work if the console of one of the 2 CMMs is configured as the modem port with **modemControlOn**.

Workaround: There is no known workaround at this time.

PR 68470

The flashsynchro operation does not remove unnecessary or obsolete files on the destination flash. Many flash synchros from CMM-A to CMM-B and back again can accumulate a large number of files.

Workaround: Delete unnecessary files on secondary CMM directories, like /flash/switch/avlan, before initiating a flash synchronization.

PR 68905

Upon reload, the switch logs the coldStartTrap instead of a warmboot trap.

Workaround: There is no known workaround at this time.

PR 69289

In **show module status** and **show ni** output, the firmware version sometimes shows up as blank.

Workaround: There is no known workaround at this time.

PR 69508

The **show cmm** command shows the bbus bridge data only. The processor data is not displayed in certain cases.

Workaround: There is no known workaround at this time.

NIs

Problem Reports

PR 59530

The check to ensure that the configured egress flood and multicast limits write to the ports bandwidth is not checked. Hence, for a 10Mbps port, the egress flood limits may exceed the actual bandwidth of the 10Mbps port.

Workaround: There is no known workaround at this time.

PR 66750

The maximum aggregate throughput for an OS8-ENI-C24 (10/100) is 2.0 gigabits/sec.

Workaround: There is no known workaround at this time.

PR 67972

The egress flood limits are not updated if the port speed is changed on OS8-ENI-C24 modules.

Workaround: Change the flood limits using CLI if the port speed is changed.

PR 68883

When the speed is changed on ENI modules (10M to 100M or vice-versa), the far end is supposed to detect this change if configured as auto. If it does not detect this condition, then the link will be down.

Workaround: Configure the far end or toggle the link status locally to restart the auto negotiation process.

Redundancy / Hot Swap

CMM Redundancy Feature Exceptions

- Manual invocation of failover (by user command or Primary pull) should only be done during times when traffic loads are minimal.
- Hot standby redundancy or failover to a secondary CMM without significant loss of traffic is only supported if the secondary is fully flash synchronized with the contents of the primary's flash.
- Failover is totally unsupported when the configuration has been changed and not saved to the working directory. In this case, the primary CMM might require a reload to get the NIs back in operating condition.

Hot Swap Feature Exceptions

- Hot swap of NIs needs to be preceded by the removal of all cables connected to the NI.
- Hot insertion of unlike modules is not supported in this release. Support is planned in next maintenance release.
- The **Reload NI** command is not supported in this release. Please use **No Power NI**/**Power NI** as an alternative.
- All insertions of NI modules cannot be followed by another hot swap activity until the OK2 LED on the inserted NI blinks green.

Hot Swap Time Limitations

- All removals of NI or SFM modules must have a 30 second interval before initiating another hot swap activity.
- All insertions of NI modules must have a 3 minute interval before initiating another hot swap activity.
- All hot swaps of CMM modules must have a 10 minute interval before initiating another hot swap, reload or takeover activity.
- All takeovers must have a 10 minute interval before following with another hot swap, reload or takeover activity.

CMM Redundancy / Hot Swap Feature Exceptions

- If you do a write memory, and do not do a certify (copy working certified) before doing a **takeover** or **reload primary**, you will lose the boot.cfg contents because the secondary will do an automatic **restore** (copy certified working) when it comes up as the secondary. This allows it to be ready for failovers.

Problem Reports

PR 66573/67300

Hot swap of an unlike NI type is not supported.

Workaround: After extracting an NI from a slot, use the same type of NI for insertion to that slot.

PR 68467

Need at least 7 MB of Free Space available on the Flash of each CMM.

Workaround: Remove unnecessary files (like bootrom.* and miniboot.* , see also directories in /flash top level). Check that the Flash capacity is correct (i.e. 32 MB).

PR 68869

The **reload** command will not work following a **debug chassis auto-reboot disable** command, even after a **debug chassis auto-reboot enable** is done.

Workaround: In a single CMM system, you need to power cycle the box. In a two CMM system, do a **reload secondary** or **reload primary** from the other CMM.

In a duplex system, user may only:

From Primary ==> **reload secondary**
From Secondary ==> **reload primary** / **takeover**

PR 68744

It is possible to do a **takeover** on the secondary while the primary is reloading due to a **reload working no rollback-timeout**.

Workaround: Do not invoke a takeover while the primary is reloading.

PR 69078

All commands which result in reloading the secondary should not be allowed while the secondary is auto-certifying the images during a flash-synchro process.

Workaround: There is no known workaround at this time.

PR 69286

Pulling out the CMM can cause software failure if not done correctly.

Workaround: While hot swapping the CMM, the pulling of the CMM must be done in a single, swift motion. After the CMM is pulled, all pins on its connector to the mid-plane should not be touching the mid-plane (or any part of it).

PR 69292

If the mac-aging time is changed from the primary CMM, the configuration is not saved, and a takeover is done, the NI will not be reset. The new value will still be reflected on the new primary CMM.

Workaround: Save the values and sync the CMMs.

PR 69319

Occasionally, on an NI hot swap, the user may see a task crash in the tIpni task.

Workaround: If this occurs, please retry the hot swap.

PR 69320

Learned Port Security configuration is lost after a takeover.

Workaround: There is no known workaround at this time.

Technical Support

Alcatel technical support is committed to resolving our customer's technical issues in a timely manner. Customers with inquiries should contact us at:

Region	Phone Number
North America	800-995-2696
Latin America	877-919-9526
Europe	+33-388-55-69-04
Asia Pacific	+65-6394-7933
Other International	818-878-4507

Email: support@ind.alcatel.com

Internet: Customers with Alcatel service agreements may open cases 24 hours a day via Alcatel's support web page at: http://eservice.ind.alcatel.com.

Upon opening a case, customers will receive a case number and may review, update, or escalate support cases on-line. Please specify the severity level of the issue per the definitions below. For fastest resolution, please have telnet or dial-in access, hardware configuration – module type and revision by slot, software revision, and configuration file available for each switch.

Severity 1 Production network is down resulting in critical impact on business - no workaround available.

Severity 2 Segment or Ring is down or intermittent loss of connectivity across network.

Severity 3 Network performance is slow or impaired - no loss of connectivity or data.

Severity 4 Information or assistance on product feature, functionality, configuration, or installation.